

10

Essential Steps to Web Security

A Clearswift Best Practice Guide



Introduction

Web 2.0 brings Threat 2.0

The web is a highly interactive, sophisticated and increasingly mission-critical platform. As online collaboration has matured and become more and more integral to many people's lives so companies are increasingly using such technologies to connect more effectively internally and externally with customers, suppliers and partners.

According to Clearswift's Web 2.0 in the Workplace Today report over half of managers see web collaboration as critical to the future success of their business. Moreover, over two-thirds of companies say that their use of Web 2.0 is allowed or encouraged within their organisation.

As businesses embrace Web 2.0 technologies - and reap benefits like cost savings, better communications and improved employee morale - it is important that enthusiasm doesn't result in ignorance of the risks. New and increasing ways to collaborate provide a greater opportunity for employees to 'mess up' and sensitive information can easily leak out to places it should never go.

Businesses must find solutions that allow them to manage threats to information security posed by increased internet usage in the workplace, while maintaining employee productivity and motivation.

Clearswift's research shows a large majority of companies recognise that a new approach to security is needed in this era of web collaboration - and we'd like to help. This short guide outlines 10 simple steps to best practice in web security. Follow them all to step up your organisation's information security and stay ahead of your competitors.

But remember that the target never stands still. Focus on the principles behind the steps - policy, vigilance, simplification, automation and transparency - and stay in touch with Clearswift to keep your information security bang up to date.



1

Policy, policy and policy.

The best web security starts with policy.

- **Policy focuses attention** - on the things you need to stop and the things you're happy to allow
- **Policy drives up compliance** - when everyone understands what's acceptable, responsible web use becomes the norm
- **Policy enforces fairness** - by making the rules clear to all
- **Policy protects** - by respecting regulations demanding due diligence

Creating a sensible policy is not difficult. Make sure everyone understands and accepts the rules and enforce the policy with technology at every gateway. Continually review the policy to stay current with changes in the way the web is used.

CLEARSWIFT SECURE Web Gateway products enforce your web security policy by filtering all web traffic in both directions. Traffic that breaches policy can be automatically blocked and reports and alerts generated.

2

Fine tune the policy

When it comes to policy, one size does not fit all. An organisation's policy should reflect the way it does business. A music company, for instance, may allow the free exchange of digital audio files. Conversely, an engineering organisation may block music downloads but allow the free flow of computer-aided design (CAD) files.

Even so, some policy rules are widely applicable:

- Block viruses
- Prevent and log spyware 'call home' activity
- Disable high-risk executable files and ActiveX downloads
- Prohibit intolerant content (such as racial or sexual discrimination)
- Restrict access to inappropriate sites (like pornographic pages and websites infected with malware)
- Stop leakage of confidential and sensitive data

With the basics sorted, it is sensible to tailor policy to fit the business. Certain departments or individuals may be afforded specific privileges or access rights, with other parts of the organisation protected by wider policy rules.

Similarly, your organisation's policy could allow certain activities during set periods. Employees may be given controlled access to social-networking sites like Facebook over their lunch break, for instance. At the same time, it could be desirable to block uploading of certain content or file types, like spreadsheets or documents that contain specific words or phrases deemed to be a risk to security.

The point is that policy should dictate your technology, not the other way around. If your filtering tools don't allow the business to operate in the way you'd like, find better tools.

CLEARSWIFT SECURE Web Gateway offers the best granular policy management in the industry. Clearswift pioneered policy-based content security and continues to lead the way.

3

Attack spyware from multiple angles

Spyware is one of the more insidious (and annoying) web hazards. Fight it from three directions:

- **Stop it at the gateway** - with automated filtering and spyware profiling
- **Stop it at the desktop** - by scanning regularly to eradicate embedded spyware
- **Stop it 'calling home'** - so newly installed spyware can't get back to base for instructions

CLEARSWIFT SECURE Web Gateway uses Sunbelt Software Border Control Anti- spyware to stop spyware at the gateway. Spyware downloads and call-homes are blocked by the award-winning CLEARSWIFT SECURE Gateways.

4

Block undesirable websites

Millions of dubious websites spring up daily. You can't keep track of them all. But technology can.

Use URL filters to block whichever kind of sites your policy demands - like gambling, pornography, remote proxies, hate sites, malware and phishing pages. Supplement the filter with a blacklist of your own, or add exceptions to a whitelist.

CLEARSWIFT SECURE Web Gateway's URL filter is supported by one of the most accurate website databases in the world. It is updated daily, with millions of sites analysed each year. The database is further enhanced by MIMESweeper, Clearswift's real-time categorisation technology. This analyses and categorises new sites and pages containing with dynamic content, aiding accurate identification.



5

Break open 'container' files

Inbound: An innocent-looking spreadsheet could carry an embedded virus. A presentation could deliver a spyware payload. A zip file could conceal any number of files that might infect your organisation's network.

Outbound: A Word document could include an embedded spreadsheet containing sensitive financial data. An apparently innocuous presentation could be a confidential company briefing. In an absent-minded moment an employee may have placed sensitive customer records information in a zip file instead of the intended fact-sheet.

Clearly, your web security must be able to decompose container files like these in order to scan for deeply embedded content. Superficial scanning may have worked five years ago. Not any more.

CLEARSWIFT SECURE Web Gateway uses deep, recursive analysis to break down all container files into their constituent parts. It then analyses and applies policy to each one independently, cleaning where necessary.

6

Watch your uploads

Companies that defend against hazardous web downloads are often vulnerable to threats travelling in the reverse direction.

Scanning email attachments isn't sufficient. Webmail services and social-networking sites present numerous ways for sensitive information and files to leak out. Elsewhere, unchecked sharing of media files saps network resources and could render your company liable for illegal use of copyrighted material.

Uploaded material has led to countless prosecutions and embarrassments. Make sure your defences are two-way.

CLEARSWIFT SECURE Web Gateway performs detection of common business terms, such as payment card industry (PCI) phrases and number patterns, personally identifiable information (PII) and compliance terms. Detection is fully customisable and is supported by automatically updated managed lists and editable compliance dictionaries, including the Gramm-Leach-Bliley Act (GLBA), Health Insurance Portability and Accountability Act (HIPAA), Securities and Equities Commission (SEC) and the Sarbanes-Oxley Act (SOX).

7

Social networking and productivity

Many companies have been quick to recognise and exploit the benefits of social-media tools to improve customer relations. Equally, employers increasingly understand that Web 2.0 tools can improve employee relations.

Staff can be happier and more motivated as a result of being allowed to use these tools in the workplace. This can in turn have a beneficial impact on business.

Balance the productivity benefits of social-networking services by including browsing schedules and time quotas in your organisation's web security policy.

CLEARSWIFT SECURE Web Gateway provides time-of-day and browse-time quota controls to enable freedom of access without the risk of abuse.

8

Monitor all web activity

That which gets measured, gets managed. Your web security should include comprehensive monitoring, reporting and analysis.

Start with big-picture snapshots of web activity. Examine the number of page requests and data volumes, for example. Then break down the analysis by user, site, activity, bandwidth, browse time and so on.

For real-time defence, set alerts to flag serious breaches before they get out of hand.

Good monitoring and reporting will let you spot suspicious activity early, revise your policy when needed and improve allocation of resources.

CLEARSWIFT SECURE Gateway solutions are famous for their rich, interactive, graphical web-based monitoring, reporting and alerting.



9

Simplify policy enforcement

Web security can encumber an entire IT department unless you simplify, automate and streamline.

Deploying, updating, managing and monitoring processes need to be designed with the real world in mind. Over-complicated or poorly integrated web security not only wastes time and resources, it weakens your defences.

CLEARSWIFT SECURE Web and Email Gateways are built around a common content-inspection engine. Policy and reporting on content, threats and user activity are then applied to all digital communication channels.

10

Innovate and grow your business

Balancing the requirement for strong network security with the need to harness collaborative web technologies is essential for business growth. Organisations need to exploit and benefit from modern web technologies and services, while ensuring that company networks remain fully protected against incoming threats and data leakage.

Develop an organisational view about new web services. Consult with key stakeholders, establish the benefits to business, understand the risks and evolve the company's usage policy accordingly.

With the CLEARSWIFT SECURE Web Gateway deployed, the web is transformed from a high-risk environment to a place of free and safe collaboration and communication. Business-enhancing online technologies like webmail, social-media websites and collaborative services can then be enabled with confidence.

Contact Clearswift

UK - International HQ
Clearswift Limited
1310 Waterside
Arlington Business Park
Theale
Reading
Berkshire
RG7 4SA
UK
Tel : +44 (0) 118 903 8903
Fax : +44 (0) 118 903 9000
Sales: +44 (0) 118 903 8700
Technical Support: +44 (0) 118 903 8200
Email: info@clearswift.com

Australia
Clearswift
5th Floor
165 Walker Street
North Sydney
New South Wales, 2060
AUSTRALIA
Tel : +61 2 9424 1200
Fax : +61 2 9424 1201
Email: info@clearswift.com.au

Germany
Clearswift GmbH
Amsinckstrasse 67
20097
Hamburg
GERMANY
Tel : +49 40 23 999-0
Fax : +49 40 23 999-100
Email: info@clearswift.de

Japan
Clearswift K.K.
7F Hanai Bldg.
1-2-9 Shibakouen,
Minato-ku, Tokyo
105-0011
JAPAN
Tel : +81 (3)5777 2248
Fax : +81 (3)5777 2249
Email: info.jp@clearswift.co.jp

Spain
Clearswift España S.L.
Cerro de los Gamos 1, Edif. 1
28224 Pozuelo de Alarcón
Madrid
SPAIN
Tel : +34 91 7901219 / +34 91 7901220
Fax : +34 91 7901112
Email: info.es@clearswift.com

United States
Clearswift Corporation
161 Gaither Drive
Centerpointe
Suite 101
Mt. Laurel, NJ 08054
UNITED STATES
Tel : +1 856-359-2360
Fax : +1 856-359-2361
Email: info@us.clearswift.com

Next steps.

Some of the ideas outlined here may seem obvious. But all organisations can benefit from reviewing their information security.

Start with your own policy. Does it reflect all of the issues explored in this document? Has everyone in the organisation read it and does everyone know where to find it? Is it continually updated to reflect new threats and activities? And, finally, do you have the right technologies in place to enforce your policy at all gateways in both directions?

If the answer is no, Clearswift can help.

Clearswift's pioneering products provide unified information security. Our company has experience in every kind of digital attack in all manner of real-world environments, from small businesses to the largest multinationals. Clearswift's solutions reflect this experience.

Talk to us about simplifying your information security without compromising. Or visit www.clearswift.com for an introduction to our unified information security products.

About Clearswift

Clearswift simplifies content security

Clearswift is a trusted information-security company with a history of innovation. We understand content and the way people work and communicate. Clearswift's content-aware, policy-based solutions benefit 17,000 organisations globally, enabling them to manage and maintain no-compromise data, email and web security across all gateways and in all directions.

Clearswift's track record in innovation includes developing many of the features the security industry now considers standard, such as image scanning, policy-based encryption and user-level message tracking. Clearswift continues to lead the IT security industry with the deployment of production-ready virtual appliances on the VMware ESX and ESXi platforms. These are built on powerful, effective and tested content-aware policies that protect our customers and their employees.

We believe that the IT security industry should evolve to help organisations interact and collaborate better in the connected world, rather than restricting communications. Clearswift's content-aware solutions reflect the mature approach that business demands, enabling safe and effective communication for unfettered productivity.

Simply, Clearswift's unified web and email security solutions dispense with fear and negativity, enabling businesses to get on with business without compromising security.